REMARKS

Claims 2-21 are pending, of which claim 2 and 8 are independent method claims with corresponding independent computer program product claims 12 and 18. As indicated above, claims 8 and 12 has been amended by this paper.[1]

The Office Action rejected each of the pending independent claims (2, 8, 12, and 18) under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,434,918 to Kung et al. ("*Kung*") in view of U.S. Patent No. 5,838,790 to McAuliffe et al. ("*McAuliffe*"). Each of the pending dependent claims was rejected under 35 U.S.C. § 103(a) as being unpatentable over *Kung* in view of *McAuliffe* or over *Kung* in view of *McAuliffe* and U.S. Patent No. 6,161,185 to Guthrie et al. ("*Guthrie*").[2]

In order to establish a *prima facie* case of obviousness, "the prior art reference (or references when combined) must teach or suggest all the claim limitations." MPEP § 2143 (emphasis added). During examination, the pending claims are given their broadest reasonable interpretation, i.e., they are interpreted as broadly as their terms reasonably allow, consistent with the specification. MPEP §§ 2111 & 2111.01.

Applicants note that for a variety of reasons, suppliers or manufacturers of certain client systems may desire to allow only selected servers to provide network resources to their client systems. Specification, p. 3, ll. 15-17. Consider, for example, a situation in which a supplier subsidizes the cost of a client system with subscription revenue based on the client system accessing network resources that the supplier provides. If the client system were to access network resources provided by a competitor, the supplier would not be able to recoup the client system subsidy, and in effect, would subsidize its competitor by providing a low cost client system to users.

As should be apparent, this problem is somewhat different from the typical scenario in which the provider of network resources, either the supplier or competitor, verifies that the client system is authorized to access the provider's network resources. While verifying that a client

---

[1]Support for the amendments may be found throughout the Specification, and particularly at page 19, lines 9-20; page 22, lines 11-22; and page 23, line 24 to page 24, line 21,

[2]Applicants reserve the right to challenge *Kung, McAuliffe,* and *Guthrie* as a proper prior art references in the future. Accordingly, any statement in this response with respect to *Kung, McAuliffe,* and *Guthrie* is made merely assuming *arguendo* that *Kung, McAuliffe,* and *Guthrie* represent prior art and should not be interpreted as acquiescing the references asserted prior art status or teachings.

system is authorized to access a provider's network resources, such as subscription-based services, can be used as a mechanism to financially support the provider's network resources, it does nothing to prevent a client system that is subsidized by a supplier from accessing a competitor's network resources. The subsidized client system need only subscribe to the competitor's network resources rather than the supplier's. Accordingly, a client system and a competitor (i.e., an unauthorized server) can collude to override conventional security systems. Specification, p. 4, ll. 8-10.

McAuliffe discloses an advertisement system. In particular, *McAuliffe* uses a key-dependent one-way hash function to generate fingerprints of both advertisements downloaded to a user's computer and an advertisement statistics file (storing statistics as to which advertisements are shown to users, for how long, and at what times) which is periodically uploaded to a remote central computer. Col. 3, ll. 42-49. The fingerprints allow for detection of any tampering with, modification of, or replacement of the advertisements and statistics file. Abstract; col. 3, ll. 49-58. Remedial action, such as disabling client software, is taken only after multiple incidents of tampering are detected within a short time period for the same user. Col. 11, ll. 4-17.

Kung discloses mutual authentication of a user and a server on a network, but without exchanging a user's password in clear text. Col. 2, ll. 16-19. The client transmits a logon ID to the server. Col. 1, ll. 53-54. The server retrieves a user password corresponding to the logon ID and uses the password to encrypt a random number. Col. 1, ll. 54-60. To decrypt the random number and authenticate the server, the user enters the password at the client. Col. 1, ll. 60-65. This random number becomes the encryption and decryption key for communication between the client and server. Col. 1, ll. 66-67. The client sends a message encrypted with the random number to the server to authenticate the user. Col. 1, l. 67 – col. 2, l. 4.

To appreciate the conventional nature of *Kung*, recognize as described above that both user and server know the password, and that the user enters the password to gain access to the server. Granted, *Kung* has improved conventional authentication in that the user's password is not exchanged in clear text, but that does not alter the foregoing observations. There is simply nothing in *Kung* to prevent the client system from subscribing to network resources offered by a competitor (an unauthorized server) of the client system supplier, and, for example, thereby deny the client system supplier the opportunity to recoup any client system subsidy. In other words,

the user can share his or her password, and thus collude, with whatever server the client system desires.

Independent claim 2 recites the limitation "decrypting the server authentication response without user interaction in order to prevent a user from colluding with an unauthorized server to circumvent server authentication." The Office Action asserts that the limitation "decrypting the server authentication response . . ." is met by the password entered at workstation (11 in Fig. 1), which is used to decrypt the encrypted password received from the server (block 35, Fig.2). For clarity, Applicants note that in *Kung* the user's password is used to decrypt a random number (also referred to as a password) that is encrypted with the user's password. The Office Action further asserts that the limitation ". . . to prevent a user from colluding with an unauthorized server to circumvent server authentication" is met by the authentication process described in blocks 33-38 of Figure 2.

While Applicants agree that *Kung* may decrypt a server authentication response, it is clear that Kung does so with user input—user input that allows a user to collude with an unauthorized server to circumvent server authentication. As described in blocks 34 and 35 of Figure 2 of *Kung*, the client workstation requests that the user enter his or her password, and the entered password is used to decrypt the encrypted password received from the server workstation. There is nothing in *Kung* to prevent the workstation from subscribing to network resources offered by any server, whether authorized to provide resources to the workstation or not. The only limitation on access in *Kung* is a password that is known to the user.

In rejecting independent claim 2, the Office Action completely ignores the portion of the limitation stating that the server authentication response is decrypted without user interaction. And, the response to Applicants' arguments is no better. The Office Action simply states that the user merely enters the password, and that there are no user actions taken in the actual decryption process. Applicants respectfully submit that whether user actions are taken during the actual decryption process in *Kung* is irrelevant. The limitation at issue reads "decrypting the server authentication response without user interaction in order to prevent a user from colluding with an unauthorized server to circumvent server authentication." *Kung* discloses that decryption of the server authentication response only occurs after the user enters his or her password, and therefore is <u>not</u> without user interaction in order to prevent a user from colluding with an unauthorized server to circumvent server authentication. In fact, it is the user's knowledge and entry of the

password that makes *Kung* susceptible to the collusion shortcoming of conventional security systems.

Accordingly, for at least the reasons stated above, Applicants respectfully submit that the cited art fails to teach or suggest all claim limitations for independent claim 2, rendering the rejection of independent claim 2 under 35 U.S.C. § 103(a) improper.

In independent claim 12, this limitation has been amended to recite "using a decryption key encoded in hardware at the client system to decrypt the server authentication response in order to prevent rogue software or operators of the client system from colluding with the server to circumvent server authentication." Although Applicants believe the arguments presented above with respect to independent claim 2 are sufficient to obtain allowance, independent claim 12 has been amended as indicated above in order to present an alternative basis for allowance to the Examiner for consideration.

Accordingly, Applicants respectfully submit that the cited art fails to teach or suggest all claim limitations for independent claim 12, and for at least the reasons stated above, request that the rejection of independent claim 12 under 35 U.S.C. § 103(a) be withdrawn.

In rejecting independent claims 8 and 18, the Office Action asserts that "disabling client functions after a number of incidents of 'tampering' in a time period" at column 11, lines 9-12 of *McAuliffe* meets the limitation of "after an allotted period of time, determining that no response to the server authentication request has been received by the client." Office Action, p. 6 (rejection of claims 8 and 18). Applicants note here that although they do not believe the amendment changed the scope of the claims, Applicants amended this limitation in their prior response to read "determining that no response to the server authentication request has been received by the client after an allotted period of time."

As point out previously, Applicants fail to see how *McAuliffe's* detecting multiple incidents of "tampering" within a short time period meets the limitation of "determining that no response to the server authentication request has been received by the client after an allotted period of time." If anything, just the opposite seems to be the case. Virtually all of *McAuliffe's* disclosure appears to be directed to detecting if tampering has occurred, none of which gives the impression of being analogous to this recited limitation. Rather than responding to Applicants' arguments, the Office Action simply includes what appears to be a cut and paste from the prior rejection. As noted in MPEP § 707.07(f), "Where the applicant traverses any rejection, the

examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it." Applicants respectfully request that the Examiner answer the substance of this argument so that the reasoning behind the rejection is clear on the record and can be addressed in the future, if necessary.

Applicants respectfully submit, therefore, based on at least the reasons indicated above, that the cited art fails to teach or suggest all claim limitations for independent claims 8 and 18, rendering the rejection of independent claims 8 and 18 under 35 U.S.C. § 103(a) improper.

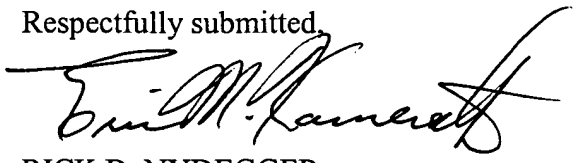
Independent claim 18 has been amended further to recite, "generating a server authentication request at the client, the server authentication request being encrypted with one or more encryption keys such that only an authorized server is able to decrypt the server authentication request." Here too, although Applicants believe the arguments presented above with respect to independent claim 8 are sufficient to obtain allowance, independent claim 18 has been amended as indicated above in order to present an alternative basis for allowance to the Examiner for consideration. Accordingly, Applicants respectfully submit that the cited art fails to teach or suggest all claim limitations for independent claim 18, and in addition to the reasons stated above, request that the rejection of independent claim 18 under 35 U.S.C. § 103(a) be withdrawn.

Based on at least the foregoing reasons, Applicants respectfully submit that the cited prior art fails to anticipate or make obvious Applicants invention, as claimed for example in independent claims 2, 8, 12, and 18. Applicants note for the record that the remarks above render the remaining rejections of record for the independent and dependent claims moot, and thus addressing individual rejections or assertion with respect to the teachings of the cited art is unnecessary at the present time, but may be undertaken in the future if necessary or desirable, and Applicants reserve the right to do so.

In the event that the Examiner finds any remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney.

Dated this 12th day of November, 2004.

Respectfully submitted,



RICK D. NYDEGGER
Registration No. 28,651
ERIC M. KAMERATH
Registration No. 46,081
Attorneys for Applicant
Customer No. 022913

EMK:kc
KC0000003003V001